DePaul University
University Libraries

DePaul Journal of Art, Technology & Intellectual Property Law

Volume 11
Issue 1 *Spring 2001*

Article 3

# A New Millennium Dilemma: Cookie Technology, Consumers, and the Future of the Internet

Courtenay Youngblood

# CASE NOTES AND COMMENTS

## A NEW MILLENNIUM DILEMMA: COOKIE TECHNOLOGY, CONSUMERS, AND THE FUTURE OF THE INTERNET

The last twelve months in the world of dot-coms and e-businesses has been a case of survival of the fittest. Unfortunately, it's been a rough road and many start-ups have not survived on the Internet. After the World Wide Web's unprecedented growth and success over the last seven or so years, some of the ingenuity and "newness" of it all has waned. Consumers have their preferred browsers and favorite Web sites they go to for conducting research, making purchases, and finding local movie listings, but have left thousands of Internet start-ups wondering where all the surfers have gone. One by one, dot-coms are faltering, watching their stock plummet, closing up shop, and answering to creditors rather than to their portfolio managers.

Let's talk about creditors for just a second. How do you suppose all of these Internet ventures that never really got off the ground – or at least out of the red – are paying for their operations sans profit? Simple, they're selling us; using the users, if you will.

Have you ever stopped to think how much money you are worth? I'm not talking about your net worth, I'm talking about your worth as a consumer. How much are you worth as Jane Smith, who lives at 2250 N. Lincoln Avenue, email address someone@email.com, who visits BestBuy.com, GolfClubs.com, and purchases electronics, toys, and books on the Internet?

Throughout the past year, hundreds of start-ups have been closing up shop and heading to court, being called as defendants in dozens of consumer privacy cases arising out of improper, and sometimes fraudulent, collection and use of Web user data. Whether it is a desperate act to save a bankrupt e-business or a profit-making scheme, some e-businesses are offering their customer databases on the auction block -- in bankruptcy or not -- to other Web companies looking for marketing opportunities. The

result has been a major backlash from consumers, the FTC, and consumer privacy groups that are now keeping a close eye on the business of customer profiling.

This article is about the "cookie" crisis – what it is and how it is affecting, and will continue to affect, the way consumers use the Internet. In the following sections, I have attempted to provide a background on the issues at play in the debate over the use of cookie technology. Section I is cookie technology in a nutshell: what a cookie is, what it does, how e-businesses are using it, and the problems Internet companies are having because they are using cookies. Section I summarizes the most significant, and currently pending, cases arising out of the alleged misuse of cookies and the claims upon which these cases are being litigated. To date, two of these cases have ended in agreed consent orders; but with more on the dockets, there is sure to be a major shift in how consumer privacy on the Internet is regulated.

Section I also provides a brief review of some of the statutes, both federal and state, that have been cited by advocates on both sides of the cookie debate. Consumer privacy and unfair trade practices statutes have been the basis of consumers' claims in these privacy suits, but often do not specifically address consumer privacy on the Internet. As a result, state and federal legislators are reevaluating existing statutes and drafting new ones that will bring these laws in line with the world of the Internet. In its first few months, the 107th Congress has been furiously drafting legislation to protect consumers' online privacy. Although neither house has passed any of the bills, this activity is a good indication of the federal government's dedication to protecting consumers.

Section II tries to make some sense of the cases, statutes, and traditional legal concepts that have been reevaluated as a result of the *DoubleClick* litigation. As recently as one year ago, it would have been a safe bet to say that few everyday users of the Internet had any idea what a cookie was, much less what it was doing on their computers. Within that same time, additional cookie-based privacy suits have been filed in state and federal courts prompting legislators and e-businesses to act. The results of these efforts are privacy standards set by e-businesses, a commitment to self-policing strategies, and the proposal by the federal government to

monitor more closely consumers' online privacy. Whether or not self-policing or government intervention will be the most feasible and most effective means of protection remains to be seen.

Finally, what has been the effect of all of this commotion on the Internet? How has our, the users' and consumers', perception and use of the Internet changed? Knowing that dozens of Internet companies have been identified for their misuse of consumers' personal information and Internet habits, may be another catalyst in what we are now seeing as a sharp decline in Internet start-up success. While the extent of the impact the cookie crisis has on the state of e-business and the digital economy is not yet certain, it is not difficult to see the dramatic impact these cases have already had on the Internet. For example, it is hard to find a Web site that does not publish a clearly identified Privacy Policy on its homepage. The privacy policy mandate arose out of one of the first cases to be litigated dealing with the cookie crisis: *In the Matter of Geocities* privacy litigation. As more cases are litigated and legislation proposed, the balance between privacy and commerce could take a swerving turn for the better, or for the worse, depending on which side you favor.

## I. BACKGROUND

Today, the Internet is estimated to have close to 168 million users worldwide, with three out of every four of these users living in North America.[1] What began as a simple research tool has become the most common and accessible way for many people to communicate, conduct business, and make purchases. As a testament to its rapidly expanding accessibility and use, the number of Web sites as of December 1999 had grown to over 9.5 million since December 1993 when there were approximately 600 Web sites in existence.[2] There are trade-offs, however, with this ease of use. The most amazing aspect of the Internet phenomenon

1 Michael S. Yang, *E-Commerce: Reshaping the Landscape of Consumer Privacy*, 33-AUG. MDBJ 12, 12 (July/Aug. 2000).

2 *Id.* at 13.

is that it provides virtually free access to almost any research, information, product, and service. Well, almost free. Lately, we Web site users are coming to find out that we are paying a hefty, non-monetary price to use the Internet; and most often, not by choice.

### *A. Who Wants A Cookie?*

Enter the "cookie." When a user enters a commercial Web site,[3] a cookie is often placed on a Web users' computer that acts as a sort of tracking device for the "owner" of that cookie. A cookie is a small piece of code a site's servers deposit onto users' computers. Once on the computer's hard drive, the cookie reports back to the Web site about that user's activity on that Web site, as well as what Web sites the user has visited since the cookie was deposited.[4] For example, Web sites can provide personalized greetings, create shopping baskets and remember passwords.[5] The cookies basically allow a business to build a database of customers' habits and hobbies -- i.e., where they created their shopping baskets and what items were in them -- by keeping track of where its customers go online after they leave its Web site.[6] This is an essentially harmless use of cookies and has not raised consumer or governmental watchdog concern.

---

3 Domain names are the registered Web addresses for Web sites on the Internet. They are identifiable by their suffixes as being most commonly supported by commercial entities (.com), government offices, committees or publications (.gov), various public service or non-profit organizations (.org), or educational institutions (.edu).

4 Robert L. MacMillan, *House Approves Anti-Cookie Amendment in Approps Bill*, NEWSBYTES NEWS NETWORK (July 21, 2000), *available at* 2000 WL 21180291.

5 Seth R. Lesser, *Privacy Law in the Internet Era: New Developments and Directions*, 607 PLI/PAT 141, at 144 (June 2000).

6 Brenda Sandburg, *Privacy Patrol*, THE RECORDER (June 28, 2000), *available at* (noting plaintiff's allegations in the *DoubleClick* litigation of secretly tracking users activity on the Internet to collect personally identifiable information).

Some companies, however, have used this information for benefits beyond their own Web sites. Consumers, consumer privacy groups, and the Federal Trade Commission are targeting companies like Geocities and DoubleClick for allegedly compiling databases of millions of consumer profiles made up of information retrieved using cookies. The data retrieved in the cookies is stored in the databases and often used by or sold to direct marketing services.

For example, Jane Smith goes to any Internet search engine. She begins her Internet search by typing the word "diabetes" hoping to locate a support group or Web site offering information about the disease and its treatment. When the browser returns the list of Web sites and pages matching her search criteria, she might notice the ad banners have changed on the top of her computer screen. They now in some way relate to diabetes: pharmaceutical companies, support groups, and any company that might use DoubleClick, as an example, as their Internet advertising agent. At this point a cookie is embedded into Jane's system and begins to track her Internet usage.

The cookie placed on Jane's computer contains a GUID, or a globally unique identifier. A GUID is a unique number that is specifically assigned to an individual Internet user.[7] DoubleClick, and presumably others like it, use this number to target the individual user and ensure that user does not see the same ad over and over again. In effect, the GUID is the main component in the cookie's tracking system: it is through this number that the Internet companies are able to identify exactly which Web sites a user has visited.[8] As Jane surfs the net and visits Web sites that are part of DoubleClick's network or clicks on ad banners that DoubleClick has placed on behalf of its clients, the GUID is transmitted back to DoubleClick.[9] Information such as the sites Jane has visited and what personal information she inputs onto various sites' pages is

7 Brett Burney, *The Double Take on DoubleClick*, SPECIAL TO LAW.COM, ¶ 12, *available at* http://www.law.com/cgi-bin/gx.cgi/AppLogic+FT Content Server?pagename=law/View&c=Article&cid=ZZZ7H3JF08C&live=true&cst=1 &pc=0&pa=0 (visited Mar. 24, 2001).

8 *Id.*

9 *See, supra* note 5, at 144.

used to compile a database of user information. The question is what are DoubleClick and other companies employing the same technologies doing with this information?

That is the same question the FTC, the Bureau of Consumer Protection, and several federal and state courts are currently trying to answer. The cookie's intended purpose is to eliminate the need for Web users to re-enter usernames and passwords each time they want to read a news article online or enter a site requiring membership. The cookie is intended to guide a Web user around the Internet. You've probably noticed that many Web sites require you to create a Login ID and password for your sessions at that site. On your first visit, you might be asked if you would like the site to remember your ID and password for future sessions. Something like, "would you like your ID and password stored on your computer for future uses?" It is this information that is stored in a cookie on your hard drive and retrieved whenever you re-visit that particular Web site. Some cookies are retrieving far more than your site visits while you are away from the Web site that placed the cookie on your system.

*In re DoubleClick* is the seminal piece of litigation in the cookie controversy because it sparked a revolution in the area of consumer privacy on the Internet. In November 1999, when news spread of DoubleClick's intentions to merge the data it had retrieved via its cookies with data stored in profiles on its Abacus Direct (a direct marketing company that is a wholly-owned subsidiary of DoubleClick) database, revelations that other companies engaging in similar practices emerged. As it turns out, the FTC had already litigated two major cases prior to the DoubleClick fiasco. Both of these cases involved Internet companies fraudulently retrieving consumer data via cookies and misusing or, in the worst scenario, selling their customer profiles to other companies for profit.

Even after Harriett M. Judnick filed her complaint against DoubleClick in January 2000, not many Web users were aware of the controversy surrounding cookies. Few e-businesses using them had clearly disclosed to Web users their commercial use of cookie technology, if at all. In fact, much of the ensuing

controversy stems from the ambiguous and convoluted privacy policies that are posted on many Web sites on the Net.

### *B. What Does the Case Law Say?*

Complaints filed in state and federal courts allege that certain e-businesses are combining consumers' personally identifiable information[10] with non-personally identifiable information[11] to compile massive databases of comprehensive customer profiles. Plaintiffs cite violations of state consumer privacy statutes, state consumer fraud and deceptive trade practices acts, and federal trade practices violations. Although some cases have been litigated, the DoubleClick litigation will likely be the most influential in the privacy debate because of the media attention it has received. The DoubleClick decision, when combined with previous FTC rulings, may guide legislators and industry executives towards effective consumer privacy protection.

#### *1. DoubleClick, Inc.*

DoubleClick, Inc. is an Internet advertising agency linked to millions of Internet users via thousands of e-business clients. In January 2000, DoubleClick publicly announced plans to combine anonymous Web user data with personal information from its Abacus Online database and other databases.[12] Explained on DoubleClick.com is that every time you see an ad delivered by DoubleClick, you are assigned a GUID which is then stored on

10 "Personally identifiable information" includes a consumer's name, address, phone number, and credit card numbers.

11 "Non-personally identifiable information" includes the data collected by cookies that indicates what sites a consumer or Internet user has frequented.

12 John T. Acquino, *Senate Online Profiling Hearing Suggests Movement Toward Federal Legislation*, E-COM. L. WKLY. (June 28, 2000), *available at* http://www.law.com/cgi-bin/gx.cgi/AppLogic+FTContentServer?pagename=law/View&c=Article&cid=ZZZGJSJZ19C&live=true&cst=1&pc=0&pa=0 (last visited Mar. 24, 2001).

your computer.[13] DoubleClick then uses that GUID to "target you" and ensure that you do not see the same ad repeatedly during your Web browsing.[14] It is both important and interesting to note that DoubleClick does not explain this process on the site where and when you are clicking an ad banner placed by them. In fact, a Web user would have to locate and read DoubleClick's Privacy Policy, or the policy of the site on which the user received the ad and cookie, to learn anything about this.

The DoubleClick cookie jar became suspicious when, in November 1999, DoubleClick completed a merger with Abacus Direct Corporation. You probably have never heard of Abacus before, but they probably know a thing or two about you. This is because Abacus runs "America's largest database of catalog-buying behavior, collecting all the purchase data from about 1100" companies that sell through catalogs.[15] On January 26, 2000, *USA Today* reported that DoubleClick, the largest advertising network on the Web, was beginning to connect users' names to their Web-surfing trails.[16] It didn't take long for privacy advocates to shift into high gear, pushing for nothing short of federal privacy protection.[17]

The plaintiff who started the cookie war, Harriet Judnick, filed her complaint on January 27, 2000 in the California Superior Court of Marin County.[18] Plaintiff charged DoubleClick with employing cookies to identify Internet users, track their Internet and Web use, and obtain personal information without their consent.[19] Plaintiff further alleged that "DoubleClick has affirmatively represented

---

13 *See, supra* note 7.

14 *Id.*

15 *Id.*

16 Elizabeth Weise, *How the Cookies Can Crumble: Ways to Block Tracking Without Government Help*, USA TODAY, Feb. 15, 2000, at 3D.

17 *Id.*

18 *DoubleClick Sued for Violating Users' Privacy Rights*, E-COM. L. WKLY. Feb. 3, 2000, *available at* http://www.law.com/cgi-bin/gx.cgi/AppLogic+FTContentServer?pagename=law/View&c=Article&cid=A15011-2000Feb2&live=true&cst=1&pc=0&pa=0 (last visited Mar. 24, 2001) (citing *Judnick v. DoubleClick, Inc.*, Calif. Super. Ct., Marin Cty., No. CIV 000421, filed Jan. 27, 2000).

19 *Id.*

itself to the public as an organization that does not collect such information" and one that "values consumers' privacy."[20] According to plaintiff's complaint, DoubleClick's acquisition of Abacus Direct Corp. in late 1999 was the final step needed for the collection of user information -- combining data retrieved via DoubleClick's cookie technology with Abacus Direct's database of American households.[21]

A judgment against DoubleClick would require the company to cease using cookies to retrieve consumer data without first obtaining the prior consent from Internet users whose information is being gathered.[22] The requested injunction would also require that DoubleClick provide consumers with an opportunity to obtain, review and destroy any personal data that the company has mistakenly gathered, as well as request that the company destroy all personal data obtained without a consumer's effective consent.[23]

The DoubleClick litigation is not the first online consumer privacy case to come before the courts, but it is the one case that has caused the most uproar. Beginning in late January 2000, a series of lawsuits were filed in several state and federal courts around the country challenging DoubleClick's alleged efforts to combine its cookie technology with the Abacus Direct database. The complaints alleged violations of 18 U.S.C. §§ 1030, 2510, et seq., and 2701, et seq.[24] State claims included Trespass to Property, Invasion of Privacy, Violation of Unfair Trade Practices Acts, Unjust Enrichment, and violation of various Consumer Protection Acts.[25] Of the twelve actions originally filed in federal court, ten were filed in the Southern District of New York. On April 6, 2000, plaintiffs in the actions filed in the Southern District

---

20 *Id.*
21 *Id.*
22 *Id.*
23 *Id.*
24 Charles L. Kerr and Oliver Metzger, *Online Privacy: Emerging Issues*, 607 PLI/PAT 29, *60 (June 2000).
25 *Id.*

of New York moved to consolidate all of those cases, and DoubleClick approved.[26]

In February 2000, the FTC and the New York Attorney General opened an informal inquiry into DoubleClick's business practices.[27] Also in February, Michigan Attorney General Jennifer Granholm initiated legal action against DoubleClick charging the company with engaging in practices similar to cyber wiretapping.[28]

On February 10, 2000, the Electronic Privacy Information Center (EPIC), a Washington-based privacy group, filed a complaint against DoubleClick, Inc. with the FTC. The complaint alleged that DoubleClick had "engaged in unfair and deceptive trade practices by tracking the online activities of Internet users and combining that tracking data with detailed personally-identifiable information" stored in their marketing database.[29] According to EPIC, DoubleClick was engaged in the assembly and tracking of consumer data with neither the knowledge nor the consent of Web users utilizing the Company's ad banners.[30] EPIC further claimed that this practice clearly violated the site's own published Privacy Policy and contradicted the many assurances that the information retrieved and maintained by the company was anonymous.[31] EPIC also alleged that DoubleClick had acknowledged that Web sites do in fact place certain information -- i.e., cookies -- on a user's hard drive "usually without their knowledge or consent."[32]

---

26 *Id.* at *61.

27 *Id.*

28 Chris Oakes, *Michigan Warns Sites on Privacy*, WIRED NEWS (June 14, 2000), *available at* http://www.wired.com/news/politics/0,1283,36967,00.html (last visited Mar. 24, 2001).

29 Mike Goodwin, *Privacy Group Files FTC Complaint Against DoubleClick Over "Cookies"*, E. COM. L. WKLY. (Feb. 24, 2000), *available at* http://www.law.com/cgi-bin/gx.cgi/AppLogic+FTContentServer?pagename=law/View&c=Article&cid=A16852-2000Feb23&live=true&cst=1&pc=0&pa=0 (last visited Mar. 24, 2001).

30 *Id.*

31 *Id.*

32 *Id.*

*2. Geocities, Inc.*

In May 1998, the Federal Trade Commission initiated an investigation of another Web site for similar misuse of customers' personally identifiable information. Following its investigation, GeoCities admitted that its practices violated various provisions of the FTC Act and agreed to certain conditions outlined by the FTC in an agreement containing consent order.[33] The FTC first alleged that the Internet Web site, which offers free and fee-based Internet services, violated its own privacy policies by selling customer information to third parties to be used in general advertising, although that information was said to be distributed only when the consumer specifically so requested.[34] Secondly, Geocities allegedly falsely represented that optional information it collected would not be disclosed without the customer's permission.[35] Lastly, the FTC charged Geocities with falsely representing that it collected and maintained personal information from children when it was actually collected and maintained by third parties via Geocities' Web site.[36]

The FTC and Geocities published the Agreement Containing A Consent Order, which the FTC believes includes the proper guidelines and policies it wants Internet companies to follow.[37] The FTC has pointed to this case as evidence of its willingness to sue Web sites that are not doing what their privacy policies and statements to consumers assure.[38] The most notable of the FTC's provisions contained in this Order requires that Geocities provide "clear and prominent notice to consumers ... with respect to respondent's practices with regard to its collection and use of personal identifying information."[39] This notice, the FTC continues, at a minimum must include: what information is being

33 *In the Matter of GeoCities*, 1998 WL 473217 (F.T.C.).

34 John C. Yates, *E-Compliance: Internet Law and Privacy Issues*, 1177 PLI/CORP 195, 206 (May-July 2000).

35 *Id.* at 207.

36 *Id.*

37 *In the Matter of GeoCities, Inc.*, 1998 WL 473217 (F.T.C.).

38 Yates, *E-Compliance*, 1177 PLI/CORP at 207.

39 *In the Matter of GeoCities, Inc.*, 1998 WL 473217 (F.T.C.).

collected; its intended uses and information advising the consumers of the ability to obtain access to or directly access such information and the means by which the consumer may do so; the means by which consumers may remove the information directly, or have it removed, from Geocities' databases; and the procedures by which consumers may delete personally identifiable information from Geocities' databases.[40]

To verify compliance with these provisions, and others outlined in the FTC's Order, Geocities was given only sixty (60) days to file a written report with the FTC "setting forth in detail the manner and form in which they have complied with this Order."[41] Last, but certainly not least, the Order's final provision stated that it will not terminate until February 5, 2019, "or twenty (20) years from the most recent date that the United States or the FTC files a complaint in federal court alleging any violation of the order, whichever comes later."[42]

According to Section 5 of the FTC Act -- the Act upon which the claims against Geocities were based -- Geocities could be fined not more than $10,000 for each violation of the Consent Order agreed to by the parties.[43] Each separate violation of the Order is deemed a separate offense; except that a continuing failure to obey the Order is measured daily, each day constituting a separate offense for the purposes of allocating fines and punishment under the Act.[44]

*3. Toysmart.com, Inc.*

In May 2000, Toysmart.com, owned largely by Walt Disney Company, stopped taking orders on its Web site devoted to

40 *In the Matter of GeoCities, Inc.*, 1999 WL 69858 (F.T.C.).
41 *Id.*
42 *Id.*
43 15 U.S.C. § 45(l) (2000).
44 15 U.S.C. § 45(l) (2000).

educational fun for kids.[45] On June 9, 2000, Toysmart.com, LLC's creditors filed a Chapter 11 petition for involuntary bankruptcy. The petition was granted by the Bankruptcy Court on June 26, 2000.[46] At the same time, however, Toysmart.com began running advertisements in newspapers seeking buyers for its assets – including its customer database.[47] At that time, Toysmart.com's database held personal and family profiles and credit card data on over 250,000 consumers who had visited the site since it first appeared on the Web.[48]

The FTC responded to Toysmart.com's solicitations for a prospective buyer with this suit. The suit was filed in the U.S. District Court (Mass.) in early July 2000 in an effort to prevent the bankrupt Toysmart.com from selling its consumer information databases.[49] The FTC believed that Toysmart.com's actual sale of its databases would violate its own privacy policies, and possibly U.S. privacy laws. By initiating legal action, the FTC believed it might be able to disrupt the company's efforts to sell the information.[50]

The FTC's complaint alleged that the company violated Section 5 of the FTC Act, 15 U.S.C. § 45(a), in its attempts to sell customer lists and profiles that included personal information provided by children using the Toysmart.com Web site.[51] Almost immediately, the FTC approved a Stipulated Consent Agreement and Final Order with Toysmart.com's owner, Walt Disney Company, contingent upon the buyer's adherence to

---

45 Brian Krebs and David McGuire, *Lawmakers Introduce Privacy Bill in Wake of Toysmart Scandal*, NEWSBYTES NEWS NETWORK (July 12, 2000), *available at* 2000 WL 21179860.

46 *F.T.C. v. Toysmart.com, LLC,* 2000 WL 1523287 (D. Mass. Aug. 21, 2000).

47 *See, supra* note 45.

48 Jerry Guidera and Frank Byrt, *Judge Refuses to Set Conditions on Toysmart Sale*, WALL ST. J., Aug. 18, 2000, at B6.

49 Press Release, Federal Trade Commission, *FTC Sues Failed Website, Toysmart.com, for Deceptively Offering for Sale Personal Information of Website Visitors*, (July 10, 2000), *available at* http://www.ftc.gov/opa/07/toysmart.htm (last visited Apr. 7, 2001).

50 *Id.*

51 *Id.*

Toysmart.com's privacy guidelines.[52] The stipulation allowed the company to sell its customer list in bankruptcy proceedings, "as long the buyer agrees to abide by the Internet retailer's previous privacy promises to safeguard the list."[53] The terms required Toysmart.com to sell the list as a package – with the Web site – and only "to a 'qualified buyer' in a related market, as determined by Judge Kenner."[54] The agreement also required Toysmart.com to delete several thousand records allegedly collected in violation of the Children's Online Privacy Protection Act of 1998, 15 U.S.C § 6501 et seq. (effective April 2000).[55]

After the FTC filed the Consent Order, thirty-nine states' attorneys general joined together to plead with Judge Kenner to block the sale because it directly violated each of their individual state's consumer privacy laws.[56] The saga continued when TrustE,[57] an Internet company that certifies e-business privacy protections, filed documents in Judge Kenner's Court in an attempt to keep the customer list from being sold.[58] Judge Kenner then expressed her concerns over the FTC's proposed agreement with Disney and Toysmart.com, and on August 18, 2000, handed down her decision.[59] In this decision, Judge Kenner set aside the conditions on the proposed sale of Toysmart.com – i.e., that the customer list be sold as a package to someone within the industry -

52 *FTC Approves Pact Allowing Toysmart's Customer List Sale*, WALL ST. J., July 24, 2000, at A28.

53 *Id.*

54 Donna DeMarco, *Web Watchdog Files Suit to Bar Firm from Selling Customer Lists*, WASH. TIMES, July 25, 2000, *available at* 2000 WL 24233242.

55 *Id.*

56 Jennifer Heldt Powell, *States Take Info Fight to Court*, BOSTON HERALD, July 21, 2000, *available at* 2000 WL 4330624.

57 TRUSTe is an Internet company that awards its seal of approval to Web sites and e-businesses who abide by certain codes of online information practices. TRUSTe also requires companies awarded their seal to submit to monitoring of their online privacy programs. There are several other companies and Web sites similar to TRUSTe as part of the massive self-regulation effort. TRUSTe and other online seal programs are discussed in Section III *infra*.

58 *See, supra* note 54.

59 Greg Gatlin, *Judge Won't OK Toysmart Pact*, BOSTON HERALD, Aug. 18, 2000, *available at* 2000 WL 4332970.

- and said the deal with regulators "only could be considered when an actual buyer for Toysmart.com's assets emerges."[60]

In its Memorandum and Order, the court stated it was "perplexed" as to why the FTC was even filing a suit against Toysmart.com, seeing as it is not a debtor in the bankruptcy proceedings.[61] The court then required the FTC to file within fifteen days of the court's order an explanation of why it was naming Toysmart.com, LLC as a defendant.[62]

*4. RealNetworks, Inc.*

RealNetworks, Inc., a software company based in the State of Washington, provides consumers with free basic versions of two products: RealPlayer and RealJukebox.[63] The products allow users to see and hear audio and video available on the Internet and to download, record, and play music.[64] Before a user can install and use either of the programs, however, they must register with the site; and this involves disclosing personal information including name, mailing and email address.[65] After registering with the site, RealNetworks assigns a GUID to each copy of the software that is downloaded and links this information to the users' name and address.[66] RealNetworks allegedly collects information that is not anonymous, but is private.

Plaintiffs Michael Lieschke, Robert Jackson, and Todd Simon accused RealNetworks of communicating with personal computers equipped with RealPlayer and RealJukebox to obtain information about the usage patterns of the computer operator.[67] Plaintiffs are

60 *See, supra* note 48.

61 *Toysmart.com*, 2000 WL 1523287, at *1.

62 *Id.*

63 *In re RealNetworks, Inc. Privacy Litigation*, 2000 WL 631341, *1 (N.D. Ill. May 8, 2000).

64 *Id.*

65 Lesser, *Privacy Law in the Internet Era*, 607 PLI/PAT at 145.

66 *Id.*

67 *Lieschke v. RealNetworks, Inc.*, 2000 WL 198424, *1 (N.D. Ill. Feb. 11, 2000).

three individuals who used defendant's products without incident until November 1, 1999.[68] At that time, the *New York Times* published an article claiming that RealNetworks was monitoring the usage habits of individuals using its software.

In order to use RealNetworks' products, plaintiffs were required to accept the site's "Agreement" and consent to its terms.[69] The Agreement, which plaintiffs did accept, made no mention of RealNetworks' retrieval of consumer data, the implantation of a cookie, or the intended use of the data retrieved. The Agreement merely informed users that RealNetworks' software will automatically communicate with the user for the sole purposes of updates, new versions, patches, bug fixes, etc., and will notify the user when this occurs.[70] Plaintiffs filed suit based on RealNetworks alleged retrieval and use of consumer data without the Web user's knowledge.

The three suits accuse Seattle-based RealNetworks of violating an array of privacy and fraud laws after the company's admission in November 1999 that it secretly used its software to record data, both personally and non-personally identifiable, from millions of Internet users.[71] The two suits filed against RealNetworks in federal courts in Philadelphia and Chicago allege that the company violated an assortment of federal laws, including computer fraud statutes and common-law privacy protections. [72] The suits follow a class action filed in Orange County Superior Court in Santa Ana last week that seeks up to $ 500 million in damages; although this particular suit accuses RealNetworks only of violating California privacy laws.[73] As of this printing, the cases were still pending.

Though DoubleClick was not the first of these cases to be filed, it was the case that brought previous consumer online privacy cases into the mainstream media.

---

68 *Id.*

69 Lieschke, 2000 WL 198424, at *1.

70 *Id.* at *2.

71 Greg Miller, *RealNetworks Breached Privacy, Three Suits Contend*, L.A. TIMES, Nov. 11, 1999, at C1.

72 *Id.*

73 *Id.*

### C. Federal and State Statutory Regulations

The body of law defining Internet users' rights to privacy is still in its infancy. In the lawsuits that have been filed thus far, various causes of action have been alleged. Some have been based on traditional legal concepts such as consumer fraud and deceptive trade practices. Others have been based on new federal statutes designed to specifically address the problems arising out of the use of the Internet. Many state legislatures are considering amendments to update the language of their consumer fraud and deceptive trade practices acts and their consumer privacy statutes. Until these amendments are enacted, suits seeking redress must rely on pre-Internet legislation. Plaintiffs have named the following federal and state statutes in most consumer online privacy lawsuits thus far.

#### 1. Existing Federal Protection of Internet Privacy

The Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030, was originally enacted in 1984 as part of a broader crime control initiative, as the first federal statute to address computer crime.[74] Congress amended the statute in 1990 "to cover all computers used in interstate commerce or communications" and "to prohibit forms of computer abuse which arise in connection with, and have a significant effect upon, interstate or foreign commerce."[75]

The most basic provision broadly defines the nature of an online privacy violation. Subsection (a)(5)(C) generally provides that, "[w]hoever ... intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage ... shall be punished."[76] Subsection (a)(5)(A) more specifically states that, "[w]hoever knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct,

74 Lesser, *Privacy Law in the Internet Era*, 607 PLI/PAT at 154.

75 *Id.*

76 18 U.S.C. § 1030(a)(5)(C) (2000).

intentionally causes damage without authorization to, a protected computer shall be punished."[77]

The CFAA, Section 1030, has been cited as a basis for the claim in some of the primary Internet privacy class action lawsuits filed recently in federal courts. The Act defines a "protected computer" simply as one that "is used in interstate or foreign commerce or communication."[78] The term "damage" means "any impairment to the integrity of available data, a program, a system, or information" that: (A) causes losses of at least $5000 during a one-year period; (B) modifies or impairs the examination, diagnosis, or treatment of any individual(s); (C) causes physical injury to any person; or (D) threatens public health or safety.[79] The penalty for a single violation or first offense of Subsection (a)(5)(C) is a fine or imprisonment for not more than one year, or both.[80]

The Electronic Communications Privacy Act (ECPA) is an amendment to the original federal wiretapping statute under Chapter 119, Wire and Electronic Communications Interception and Interception of Oral Communications.[81] The Act is "the primary legal protection against the unauthorized interception, use or disclosure of electronic communications while in transit or in storage."[82] Though none of the class action lawsuits discussed *supra* alleged violations of the ECPA, the Act contains two substantive provisions applicable to consumer online privacy litigation.[83]

One article suggested private plaintiffs basing claims on defendants' use of cookies might successfully raise an ECPA claim by alleging that defendants' actions actually intercept communications between consumers' computers and Web sites.[84] Advocates of the ECPA assert that this constitutes a violation of § 2511(a), which states that "any person who intentionally

77 18 U.S.C. § 1030(a)(5)(A) (2000).
78 18 U.S.C. § 1030(e)(2)(B) (2000).
79 18 U.S.C. § 1030(e)(8) (2000).
80 18 U.S.C. § 1030(b)(2) (2000).
81 18 U.S.C. § 2510, et seq. (2000).
82 Lesser, *Privacy Law in the Internet Era*, 607 PLI/PAT at 158.
83 *Id.*
84 *Id.* at 157.

intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication ... shall be punished ... or subject to suit."[85] Plaintiffs asserting an ECPA claim, however, must prove that the defendants' behavior was intentional.

Defendants may also raise an affirmative defense to an invasion claim under § 2511. Subsection (2)(d) provides:

> [I]t shall not be unlawful under this chapter for a person not acting under color of law to intercept a wire, oral, or electronic communication where such person is a party to the communication or where one of the parties has given prior consent to such interception unless such communication is intercepted for the purpose of committing any ... tortious act in violation of the Constitution or laws of the United States or of any State.[86]

The statute, therefore, leaves open the possibility that interception may be permissible if "consent" is interpreted to mean the acquiescence of a Web user to the terms of an e-business' privacy policy or of a licensing agreement posted on the Web site.[87]

It is apparent from the existing statutes that consumers are left with minimal recourse against online privacy invasion under current federal laws. Since the DoubleClick made headlines over one year ago, legislators have begun drafting bills to address protection of consumer privacy. None of these bills has been passed by either house of Congress, but there mere existence is an encouraging sign of the federal government's dedication to consumer privacy protection. In the meantime, consumers will have to rely on the broad language of Section 5 of the Federal Trade Commission Act (FTC Act), making it unlawful for one to

85 18 U.S.C. § 2511(a) (2000).
86 18 U.S.C. § 2511(d)(2) (2000).
87 *Id.*

engage in "unfair or deceptive acts or practices in or affecting commerce."[88]

*2. State Consumer Fraud and Deceptive Trade Practices Acts*

Plaintiffs filing suit in state courts most often allege violations of state consumer fraud and deceptive trade practices acts. Every state has a statute similar to the Federal Trade Commission Act that protects consumers from deceptive and unfair trade practices.[89] Unlike the FTCA, some state statutes do specifically provide for private consumer actions,[90] some even permitting plaintiffs to recover attorneys' fees and varying degrees of damages (punitive, treble or minimum).[91]

There have been few state court decisions giving some insight into how courts may view such activity. In Illinois, for example, at least one court has held that an offline practice similar to online profiling violates a state consumer fraud law.[92] In *Dwyer v. Amer. Express Co.*, the court held that "the failure of a credit card company to inform card holders that their spending habits would be analyzed and their names sold to advertisers" constituted a deceptive trade practice under the Illinois Consumer Fraud Act. [93] The court, however, fell short of citing defendant credit card companies for violating credit card holders' rights of privacy.

88 15 U.S.C. § 45(a)(1) (2000).

89 Lesser, *Privacy Law in the Internet Era*, 607 PLI/PAT at 160 (*See, e.g.*, N.Y. Gen. Bus. Law. § 349, et seq.).

90 *Id.* at 170.

91 *Id.* at 162.

92 *Id.* at 160-161.

93 *Dwyer v. Amer. Express Co.*, 652 N.E.2d 1351, 1357 (1st Dist. 1995) (holding that, under the Illinois Consumer Fraud Act, defendants did not violate card holders' rights of privacy but were engaged in deceptive practices upon which consumers relied).

*3. Common Law Consumer Privacy*

States lacking statutes to address online profiling are referring to traditional consumer protection law. For example, Michigan Attorney General Jennifer Granholm used a decades-old consumer protection law in her attack against online privacy violations. In February 2000, Granholm served "notices of intended action" on behalf of the state to four web sites - Stockpoint.com, Procrit.com, AmericansBaby.com, and iFriends.net [94] In the notices, the Michigan Attorney General charged each company with failing to disclose to consumers its information collection practices, violating Michigan's Consumer Protection Act.[95]

Illinois' own Consumer Privacy Act prohibits a "communications company" from installing or using any equipment which would allow a communications company to "visually observe or listen" to what occurs within an individual "subscriber's" household.[96] For the purposes of this statute, a "communications company" means any person or organization that "owns, controls, operates or manages any company which provides information or entertainment electronically to a household."[97] This definition specifically includes, but is not limited to, a cable or community antenna television system.[98] Without more specific state consumer protection laws, it is only a matter of time before plaintiffs fail to sustain their consumer privacy claims against e-businesses as "cable systems."

## II. ANALYSIS

Until the DoubleClick litigation hit the headlines, the average Internet user was oblivious to companies' efforts to collect and sell

94 *See, supra* note 28.
95 *Id.*
96 720 ILL. COMP. STAT. ANN. 110/3-3(a) (West 2001).
97 720 ILL. COMP. STAT. ANN 110/2 (West 2001).
98 *Id.*

consumers' Internet habits.[99] It wasn't until January 2000 that consumers began to learn that their wanderings on and offline left an electronic trail that might be sold to businesses. The full impact of DoubleClick, and others charged with similar violations, remains to be seen.

What we have seen are the reactions from the e-business community, state and federal legislators, and administrative agencies like the Federal Trade Commission to consumers' fears and allegations of fraud and abuse. In fact, a study published in November 2000 confirmed the rate of Internet companies going out of business is accelerating, with the "dot-com death count" now standing at 130 for the year.[100] Some 75 percent of "dot-bombs" cited by the study were consumer businesses, and 60 percent were e-commerce companies.[101]

Since I began researching the DoubleClick case, several steps have been taken to address the problems and resolve the litigation before it costs businesses and consumers even more. State and federal legislatures have been churning out dozens of proposals to create and clarify consumer privacy rights and other laws governing the Internet.[102] The 107th Congress has proposed at least three bills since January 2001 dealing with consumers' online privacy rights. Just months after the media picked up on the DoubleClick litigation, the ad giant reversed its course and stated that it would not link people's names, addresses, and other personal information with the data it collects during users' travels through cyberspace; at least not until government and industry set privacy standards. [103] The real questions are what does it all mean, and will any of these remedies really work?

---

99 Lesser, *Privacy Law in the Internet Era*, at 143.

100 *New Study Counts 130 Dot-com Shutdowns This Year*, ZDNET NEWS, ¶ 1 (Nov. 16, 2000), *available at* http://www.zdnet.com/ecommerce/stories/0,10475,2655286,00.html (last visited Mar. 24, 2001).

101 *Id.*

102 Lesser, *Privacy Law in the Internet Era*, at 149-153.

103 Andrea Petersen, *DoubleClick Reverses Course After Privacy Outcry*, WALL. ST. J., Mar. 3, 2000, at B1.

### *A. Industry Standards or Government Initiative?*

Since the beginning of 2000, state and federal governments have been rallying behind countless legislative proposals which seek to somehow curb this formidable rise in cookie litigation.[104] Although consumers were actually the first to file formal litigation, regulatory and administrative agencies like the FTC have begun drafting and implementing privacy standards that apply to the collection and use of personally identifiable information retrieved online.

#### *1. Are Industry Standards Enough?*

The government *and* the Internet industry have strongly stated their preferences for industry self-regulation to deal with the online privacy situation. Whether the guidelines are created and enforced by the industry itself or are a combination of both government and industry effort, consumers just want to be reassured that their identities are safe – on and offline.

The main group working to promote comprehensive industry guidelines for Internet privacy is the Online Privacy Alliance (OPA). Its Web site defines the group as "a diverse group of corporations and associations who have come together to introduce and promote business-wide transactions that create an environment of trust and foster the protection of individuals' privacy online."[105] In order to join and remain a member of the OPA, each member organization (e-business) must agree that its policies for protecting personally-identifiable information in an online or electronic commerce environment will address at least the following

104 *See, supra* note 102 and accompanying text.

105 Online Privacy Alliance, http://www.privacyalliance.org/members (last visited Mar. 10, 2001). These principles are the precise guidelines set forth by the FTC in its Consent Order in *In re Geocities* in 1998. The FTC has stood by these guidelines as those to which all Web site operators should adhere in collecting and using consumers' information.

elements, and leave room for customization and enhancement of these principles where needed.[106]

First, each member organization must adopt a Privacy Policy that is clear and concise in its terms and explanation of data collection practices and privacy principles. Secondly, the Policy must be posted conspicuously on the organization member's Web site and, overall, easy to read, find, and understand. Finally, the member-site's policy must state clearly: (1) what information is being collected; (2) the purpose for which the information will be used; (3) possible third-party distribution of that information; (4) the choices available to an individual who opposes the collection, use and distribution of the collected information; (5) a statement of the organization's commitment to data security; and (6) what steps the organization takes to ensure data quality and access.[107]

The government has been promoting self-regulation since 1995, in part by hosting a series of Internet privacy workshops geared towards educating industry groups and trade associations on the issues they face.[108] In addition, the FTC has recently requested that these groups and associations voluntarily submit copies of their online information practice guidelines and principles to further its efforts to facilitate self-regulation.[109] While this is not necessarily "industry standard," it is certainly a step in the right direction. The strength and success of the Internet, and the World Wide Web as a whole, depends on collaboration – between government, business, and consumers.

### *B. Self-Policing: Privacy Policies and Privacy Seal Programs*

In December 1999, the Electronic Privacy Information Center published a report on Internet privacy policies addressing the fact

106 *Privacy Protection Guidelines*, Online Privacy Alliance *available at* http://www.privacyalliance.org/resources/ppguidelines.shtml (last visited Mar. 12, 2001).

107 *Id.*

108 Kerr & Metzger, *Online Privacy*, 607 PLI/PAT at 32.

109 *Id.*

that these policies did not adequately address privacy issues.[110] EPIC reviewed over 100 of the most popular online shopping sites to assess their privacy policies and whether these sites were protecting consumer privacy.[111] EPIC discovered that privacy policies were confusing and inconsistent, and lacked many of the FTC's disclosure and notice requirements.[112]

This lack of substance may be why the "Privacy Seal Programs" offered by TRUSTe and BBB*Online* – the two main programs of this type – have become benchmarks for consumer privacy advocates. The programs independently assess, monitor, and evaluate members' sites and privacy policies to ensure that both remain within the program's principles and guidelines. Both TRUSTe and BBB*Online* list hundreds of members who have met the membership requirements. The EPIC report is a good benchmark for determining whether e-business self-regulation is feasible. If e-businesses cannot produce clear and comprehensible privacy policies on their own sites, are we to expect that they are adhering to the FTC's more specific guidelines for consumer privacy?

*1. E-Business Privacy Policies*

The December 1999 report published by EPIC is actually the third of its kind. Gradually increasing in scope and modifying its focus on online privacy issues, this latest installment specifically focused on the adequacy of the language, location, and comprehensibility of the Privacy Policy itself.[113] EPIC found that a February 2000 survey confirmed that "less than 10 percent of Web sites offer a baseline privacy policy," even though self-regulation continues to govern privacy protection on the Web.[114]

110 *Surfer Beware III: Privacy Policies without Privacy Protection*, EPIC, ¶ 1 (Dec. 1999), *available at, http://www.epic.org/reports/surfer-beware3.html* (last visited Apr. 7, 2001).

111 *Id.*

112 *Id.*

113 *Id.*

114 *Id.*

EPIC examined the following factors to determine the effectiveness of a site's privacy policy: (1) whether personally identifiable information was collected; (2) whether a policy was clearly displayed on the homepage; (3) whether a policy was displayed on all pages on which personal information was collected; (4) whether the site was part of a licensing group such as TRUSTe or BBB*Online*; (5) whether the site required opt-in consent for collection and later use of any and all personal information; (6) whether the site allowed users to view and correct personal information; (7) whether the use of personal information was limited in scope; and (8) whether the policy clearly specified the purposes for which personal information was collected and used.[115] The EPIC study found that though most Web sites had clearly posted privacy policies, they were utterly confusing or lacking in any meaningful protection for consumers.[116]

### *2. Third-Party Privacy Seals and Programs*

In the last year, online seal programs have become extremely important and popular with both consumers and e-businesses. Just as consumers look to the Good Housekeeping Seal of Approval on household goods or the Underwriters' Laboratories' (UL) listing on electronics as built-in safety stamps, so have Internet users come to trust various third-party seals. TRUSTe and *BBBOnLine* give their seals to Web sites that have comprehensive privacy policies and agree to adhere to the programs' principles on privacy monitoring and regulation.

*BBBOnLine* is a wholly owned subsidiary of the Council of Better Business Bureaus.[117] Its mission is "to promote trust and confidence on the Internet" through the BBB*OnLine* programs for businesses: Reliability Seal Program and Privacy Seal Program.[118]

---

115 *Id.*

116 *Id.*

117 *Welcome to BBBOnLine*, BBB*OnLine*, *available at* http://www.bbbonline.org (last visited Mar. 20, 2001).

118 *Id.*

BBB*OnLine*'s Privacy Seal Program supervises participants and their adherence to the Program's "responsible information practices."[119] The group stands by its motto for all participating companies to "say what you do, do what you say, and have it verified."[120] BBB*OnLine* participants' main goal is to promote the trust and confidence necessary for the future success of the Internet.

Based on the Better Business Bureau's own expertise in self-regulation and dispute resolution, BBB*OnLine* requires "verification, monitoring and review, consumer dispute resolution, a compliance seal, enforcement mechanisms and an educational component" to comply with the Program.[121] Though privacy programs are intended to increase consumers' comfort on the Internet, participation in them has become more like a requirement for any e-business wanting to survive under this microscope.

TRUSTe is another online privacy seal program promoting consumer privacy and helping e-businesses to maintain a secure Web site for consumers. A cornerstone of the TRUSTe program is its "trustmark," an online branded seal displayed on member Web sites.[122] TRUSTe's awards its trustmark to only those sites that: (1) adhere to established privacy principles, and (2) agree to comply with continuous TRUSTe oversight and consumer resolution procedures.[123]

The U.S. Department of Commerce, the FTC, and prominent industry associations have given their overwhelming support of TRUSTe's program principles. The principles include: (1) adoption and implementation of a privacy policy that addresses consumer anxiety over sharing personal information online; (2) notice and disclosure of information collection and use practices; (3) giving consumer's the choice and opportunity to exercise

---

119 *About the Privacy Program*, BBB*OnLine*, *available at* http://www.bbonline.org/privacy/index.asp (last visited Apr. 10, 2001).

120 *Id.*

121 *Id.*

122 *The TRUSTe Program: How it Protects Your Privacy*, TRUSTe, *available at* http://www.truste.org/consumers/users_how.html (last visited Mar. 20, 2001).

123 *Id.*

control over their personal information; and (4) data security and quality measures to help protect the security and accuracy of personally identifiable information.[124]

Web sites displaying the TRUSTe trustmark must disclose their personal information collection practices in a privacy policy statement that is clear, concise, and available from a link on the site's homepage. TRUSTe offers guidelines and samples to e-businesses drafting online privacy policies modeled after the Geocities Consent Order.[125] A significant benefit of the program is that consumers believing a trustmarked site has violated its own privacy policy can file a complaint directly from the violator's site. The "Watchdog Form" is an "online mechanism for reporting violations of posted privacy policies, specific privacy concerns pertaining to TRUSTe Web site licensees, or misuse of the TRUSTe trustmark."[126]

These privacy seal programs ease consumers' fears about logging onto the Internet, and divulging anything from a login ID to an address or credit card number. Unfortunately for consumers, there are far fewer seals than one would hope and expect to see on the Web in the aftermath of the DoubleClick backlash. In fact, TRUSTe lists only a few hundred Web sites that they consider licensees.[127] It remains to be determined whether self-regulation is adequate to protect consumers' online privacy.

## III. IMPACT

In light of the case law and statutes applied in the most recent round of litigation, where do we go from here? The law governing the Internet is still in its infancy. With the explosion of the Internet and the growth and development of the e-business culture, traditional legal concepts are extremely difficult to apply to the

124 *Id.*

125 *See Id.*

126 *The TRUSTe* Watchdog, TRUSTe, *available at* http://www.truste.org/users/users_watchdog.html (last visited Mar. 20, 2001).

127 *See, Look Up A Company*, TRUSTe, *available at* http://www.truste.org/users/users_lookup.html (last visited Mar. 20, 2001).

World Wide Web. Currently, plaintiffs are basing their claims on traditional legal concepts that are often stretched in an attempt to cover the violations alleged. State claims are generally based on consumer protection statutes, invasion of privacy, trespass to personal property or chattel, and state constitution articles and provisions. These old statutes, however, cannot possibly address the issues raised by a world now moving at the speed of the Internet.

### *A. What's Next For Consumers and E-Businesses?*

On the heels of the cases recently decided and others now before the courts, state legislatures have finally begun to reevaluate statutes in order to consider regulation of e-commerce and its impact on privacy. Most notable are the initiatives proposed by the National Association of Attorneys General (NAAG). In a March 28, 2000 letter, the NAAG expressed its concern that the lack of clear rules concerning how personally identifiable consumer information will be treated on the Internet by e-businesses "is one of the biggest threats to the longevity and vitality of electronic commerce."[128]

Consumers and Web site operators are now left wondering how to approach the issues raised by cookies. In Sections I and II of this article, I discussed and analyzed the case law, state and federal statutes, and various self-regulation initiatives at issue in the Internet privacy debate. Many Internet users know little about cookie technology and how it is used, but have come to realize there is a price to pay for Internet freedom. What exactly is that price? Am I comfortable seeing direct mail with my name, address, etc. on them, and having no absolutely no idea how this company or person got my name and address in the first place? Are most Internet users as oblivious to this as I was? Probably, and unless Web site operators and e-businesses make more of an effort to inform consumers, their demise may be sooner than they think.

---

128 Kerr & Metzger, *Online Privacy*, 607 PLI/PAT at 42.

### *B. Addressing Consumers' Concerns*

E-businesses and the government are now making concerted efforts to rewrite the law books to address the issues cyberspace has presented. As more complaints were filed against DoubleClick,[129] Alexa Internet,[130] and Yahoo, Inc.,[131] federal legislators began addressing online privacy with a hoard of proposed legislation.[132] In response, there has been a flurry of activity in the public and private sectors to protect Internet users from involuntarily divulging personally identifiable information while they surf the Web. Dot-com companies are readying new services that raise new privacy concerns, while others are changing or adding privacy policies a mile long.[133] At the same time, however, the government and dot-com companies are developing proposals, protocols, and software programs to address the issues and concerns.[134] What impact has this had on traditional legal concepts and the development of cyberlaw?

#### *1. Legislative Proposals*

The 107th Congress has been extremely busy during the first few months of 2001. Already it has introduced at least three bills that specifically address consumers' online privacy and disclosure. Though none have passed either house of Congress, their mere

129 *Healy v. DoubleClick, Inc.*, 00 Civ. 0641 (NRB); *Donaldson v. DoubleClick, Inc.*, 00 Civ. 0696 (RMB); *Wong v. DoubleClick, Inc.*, 00 Civ. 1290 (RMB).

130 *Newby v. Alexa Network and Amazon.com, Inc.*, No. C 00-0054 (N.D. Cal. filed Jan. 6, 2000); *Bieles v. Alexa Internet and Amazon.com, Inc.*, No. C 00 0187 (N.D. Cal. filed Jan. 14, 2000); *Supnick v. Amazon.com, Inc.*, No. C-00 0221-p (W.D. Wash. filed Jan. 6, 2000).

131 *Stewart v. Yahoo, Inc., et al.*, No. 00-010405 (Tex. Dist. Ct., 162 Jud. Dist. filed Feb. 12, 2000) (plaintiff alleges that Yahoo! violated Texas' antistalking laws by placing cookies on her computer and observing what sites she surfs.).

132 Kerr & Metzger, *Online Privacy*, 607 PLI/PAT at 51.

133 Thomas E. Weber, *To Opt In or Opt Out: That is the Question in the Privacy Debate*, WALL ST. J., Oct. 23, 2000, at B1.

134 *Id.*

existence is significant proof that the federal government will not wait for self-regulation to calm consumers' fears.

On January 29, 2001, the Senate introduced a bill "to provide for the disclosure of the collection of information through computer software."[135] The proposed legislation would require any computer software made available to the public, with the capability to collect and maintain information about the user, to comply with specific notice requirements. For example, the software would be required to include: (1) clear notice that it contains such capabilities; (2) a description of the information subject to collection; and (3) clear electronic instructions on how to disable such capability without affecting software performance or function.[136]

The Consumer Online Privacy and Disclosure Act, H.R. 347, was introduced in the House on January 31, 2001. If passed, this legislation would require the FTC to prescribe specific regulations "to protect the privacy of personal information collected from and about individuals on the Internet, and to provide greater individual control over the collection and use of that information."[137] The proposed legislation would make it unlawful for any operator of a Web site or online service to collect, use, or disclose personal information concerning any individual over 13 years of age, in a manner that violates specific FTC regulations.[138] Though it does not specifically state as much, the "specific FTC regulations" closely resemble those outlined by the FTC's 1998 Geocities Order. The House also introduced the Privacy Commission Act on February 13, 2001 to establish a commission for "the comprehensive study of privacy protection," though no specific details have been released.[139]

---

135 Spyware Control and Privacy Protection Act of 2001, S. 197, 107th Cong. (2001).

136 *Id.*

137 Consumer Online Privacy and Disclosure Act, H.R. 347, 107th Cong. (2001).

138 *Id.*

139 Privacy Commission Act, H.R. 583, 107th Cong. (2001).

*2. Self Regulation: The NAI*

The potential for online abuse stemming from the cookie scare prompted several federal agencies into considering regulations to limit their use. In November 1999, the FTC and the U.S. Department of Commerce jointly sponsored a Public Workshop on Online Profiling.[140] In an effort to prevent them from developing regulations limiting the development of consumer databases, eight major Internet advertising companies worked with the FTC and developed self-regulatory rules that limit how and when online consumers' actions may be traced and recorded by e-businesses.[141] The rules were just given the okay by the FTC in late July and are now in effect.[142]

The companies responsible for developing the new rules collaboratively called themselves the "Network Advertising Initiative" and included 24/7 Media, AdForce, AdKnowledge, Avenue A, Burst! Media, DoubleClick, Engage, and MatchLogic.[143] "Before the new rules took effect, Web companies had few guidelines as to when and how they could use [cookies and] online profiling to build databases about their customers."[144] The result of their efforts is four principles that are to serve as the basis for protecting consumer privacy in this area.

First, the rules provide that Web sites must clearly and unambiguously notify customers of network advertisers' profiling activities and offer consumers the choice not to participate in the profiling.[145] If personally identifiable information is collected, "robust" notice will be required before the personal data is even

140 *Federal Trade Commission Issues Report on Online Profiling*, FTC (July 27, 2000), *available at* http://www.ftc.gov/opa/2000/07/onlineprofiling.htm (last visited Apr. 7, 2001).

141 Mark Grossman & Bradley Gross, *Online Profiling: Good Business or None of Your Business?*, LEGAL TIMES Sept. 19, 2000 at 29.

142 *Id.*

143 *See, supra* note 140.

144 Grossman & Gross, *Online Profiling*, LEGAL TIMES Sept. 19, 2000 at 29.

145 *See, supra* note 140.

entered.[146] Customers will then be notified beforehand if any information such as names, addresses, or telephone numbers is being collected. For Web sites seeking to retrieve non-personally identifiable information, or "clickstream" data collected for profiling, "clear and conspicuous notice" will be in the host Web site's privacy policy.[147] Most importantly under the Principles is the provision that NAI companies contractually require host Web sites to provide these disclosures and will make reasonable efforts to enforce these notice requirements.[148]

The second NAI Principle concerns consumer choice: customers must be given a choice on participation in profiling.[149] Once informed about the network advertiser's information collection practices, consumers must be given the opportunity to decide whether to participate. The "choice" method depends on "the type of information collected and the consumers' knowledge about, and level of control over, the original collection of information."[150]

The crux of the privacy litigation is the combination of a Web user's non-personally identifiable data with his or her personally identifiable information. What Web sites Jane Smith visited on October 29, 2000 means much more to an e-business when combined with Jane's personally identifiable data retrieved by that site at an earlier date – perhaps when she made an online purchase and entered her name, mailing and email addresses, and phone number. Under the NAI Principles, if a business wants to link Jane's personally identifiable information that it already knows with the fact that Jane just visited HomeFurniture.com, the customer must first affirmatively consent ("opt-in") to this procedure.[151] If the e-business simply wants to link non-personal

146 *Id.* "Robust" notice is explained by the FTC's Opinion as notice "appearing at the time and place of information collection."

147 *Id.*

148 *Id.*

149 *Id.*

150 *Id.*

151 This is the procedure now known as "opt-in." After a consumer or Web user has been properly informed of that site's information collection practices, the consumer may give his or her affirmative consent to continue using the site; with the knowledge that his or her data is being collected.

data about Jane, it has to give her the opportunity to "opt-out" before doing that.[152]

Third, the NAI Principles promise that consumers will be given reasonable access to personally identifiable and other information that is kept by a network advertiser for profiling.[153] This is likely to wreak havoc on smaller e-businesses already struggling to make profits in the dot-com business world. This Principle may mean that businesses spend significant amounts of time, labor, and money creating and maintaining massive customer databases that store the information customers have opted-in. A customer given reasonable access to his customer profile will mean that companies will need to run a search of the entire database upon the request of the consumer – a task that could take days of manpower and resources. One commentator has suggested that in the coming months we might see several software solutions introduced to allow compliance with the access requirement without over-burdening the small or mid-size e-business that does not have the manpower or financial resources to run these searches.[154]

Finally, the NAI Principles require reasonable efforts on behalf of the advertisers to protect data they collect for profiling purposes from loss, misuse, alteration, destruction, or improper access.[155] This rule will probably be the least controversial because most companies have some system already in place to protect the data from loss, misuse, improper access, and the like. I find it interesting, however, that "misuse" is not defined in light of the confusion over the multitude of changes made to privacy policies across the Internet since the DoubleClick litigation broke the headlines.

Jodie Bernstein, Director of the FTC's Bureau of Consumer Protection, stated, following the FTC's approval of the NAI's principles, "I applaud their willingness to take significant steps in this area, and hope that the entire online industry follows their

152 "Opt-out" technology provides the consumer the opportunity to be prompted at each point of data collection and choose at each of those points whether to allow the site to collect his or her data.

153 *See, supra* note 140.

154 Grossman & Gross, *Online Profiling,* LEGAL TIMES Sept. 19, 2000 at 29.

155 *See, supra* note 140.

lead."[156] There is still, however, much work that needs to be done. Falling short of calling this the result that was needed to resolve the Bureau's and the FTC's concerns, Ms. Bernstein stated that there is still a strong need for legislative action in this area. She recognized that although the NAI constitutes over 90% of the network advertising industry, "[l]egislative action is necessary to ensure the remaining 10% will comply with the protections outlined in NAI's Principles and to guarantee full compliance by all Web sites."[157]

If this is the case and most dot-coms comply with them, the NAI Principles should alleviate at least some consumer concerns. As Ms. Bernstein said, however, there is still a strong need for legislative action in this area. While the NAI looks to be strongly dedicated to its purposes and goals, there is still that fear of the poodle, home alone, watching over the valuables. More strength is needed to stand behind the poodle and protect consumers' fears in order for us, the users that actually drive dot-coms, to continue to shop online and divulge our most personal information. There is hope that some of the proposals listed below may find there way through the new Congress and onto the statute books.

*3. Beyond Self-Regulation*

Currently in the United States there are no general privacy laws that apply to all websites, and the FTC's enforcement powers are limited to exceptional cases.[158] Because this was an election year, there was a flurry of activity by various senators and representatives to introduce legislation dealing specifically with consumers use and privacy on the Internet. Over the course of the last eleven months, various versions of legislative proposals have been submitted in an attempt to define and outline what it means to

156 *Id.*

157 *Id.*

158 Declan McCullagh and Nicholas Morehead, *FTC Goes Public with Privacy*, WIRED NEWS NETWORK, Dec. 10, 2000, *available at* http://www.wired.com/news/politics/0,1283,37695,00.html (last visited Apr. 7, 2001).

provide consumer privacy on the Internet. None of these, however, have been passed by Congress – other than the Children's Online Privacy Protection Act, discussed *supra*.

Also during the past year, a group of programmers, working together as the World Wide Web Consortium, or W3C, developed a protocol designed to enhance online privacy.[159] The standard protocol, which has been dubbed P3P for Platform for Privacy Preferences, is designed to provide Internet users with the option of selecting the type of privacy policy they wish to use.[160] According to the P3P, a web server would automatically communicate how it collects and shares data with other Web site operators or companies capable of collecting the data.[161] The protocol would then "instruct" a user's browser to only go to those sites that meet its privacy specifications.[162] While some privacy advocates believe the self-regulation is superior to a legislative fix, others have said that the P3P does not adequately protect consumers' privacy.[163] We are therefore left in the same position we were prior to Harriet Judnick's complaint – Web users and consumers remain unaware of exactly what information is being collected from them and where exactly it is going.

## IV. CONCLUSION

DoubleClick was caught off-guard by the consumer backlash that ensued after that fateful press release. It seemed that DoubleClick was in right place both at the right and wrong time. The company was one of the first to see the potential of Internet advertising, and today it provides advertising to a majority of the

159 Sandburg, *Privacy Patrol*, The Recorder, June 28, 2000, *available at,* http://www.law.com/cgi-bin/gx.cgi/Applogic+FTContentServer?pagename=law/view c =Article cid=ZZZNUGW50AC live=true cst=1 pc=0 pa=0 (last visited Apr. 7, 2001).

160 *Id.*

161 *Id.*

162 *Id.*

163 *Id.*

most frequently visited Web sites.[164] Its success hinged on the use of cookie technology to track site users' habits, better determining what advertisements should display with each user. However, when news broke of the information that was allegedly being collected by DoubleClick's cookies, the company quickly became "the poster child for privacy abuses on the Internet."[165]

It is important to note that cookies have many positive benefits to Web users, including the ability to customize a user's Internet experience by "remembering" the sites last visited and streamlining transactions by maintaining personal information. DoubleClick got into trouble because it announced plans to connect online cookies to an offline user; but then quickly abandoned these plans in the face of a fast and furious consumer backlash.

As this article was being published, U.S. District Judge Naomi Rice Buchwald of the U.S. District Court for the Southern district of New York dismissed plaintiff's class action lawsuit against DoubleClick, Inc. for failing to state a viable claim.[166] On March 29, 2001, Judge Buchwald held that DoubleClick's practices of placing cookies on a computer user's hard drive does not violate the Electronic Communications Privacy Act ("ECPA"), 18 U.S.C. § 2701, et. seq., the Wiretap Act, 18 U.S.C. § 2510, et. seq., or the Computer Fraud and Abuse Act, 18 U.S.C. § 1030, et. seq.[167] In dismissing plaintiffs' ECPA claim, the court explained that, for purposes of statutory interpretation, a visit to a web site is actually a communication between that web site and the computer user.[168] The court held that, as a matter of law, DoubleClick affiliated web sites were "users" of Internet access under the ECPA, therefore "[a]ll that the web sites must authorize is that DoubleClick access plaintiffs' communications to them."[169]

---

164 Jones, Day, Reavis & Pogue, *DoubleClick and the Privacy Wars*, MONDAQ BUS. BRIEFING, Aug. 8, 2000, *available at* 2000 WL 9238748.

165 *Id.*

166 In re DoubleClick Privacy Litigation, 2001 U.S. Dist. Lexis 3298 (S.D.N.Y. Mar. 29, 2001)

167 Id. at *1.

168 Id. at *33.

169 Id. at *35-36.

Although Judge Buchwald determined that DoubleClick was not guilty of collecting users' personally-identifiable information and creating database profiles, it does not mean that the potential threat of the harm has not been eliminated. The FTC Commissioner, Orson Swindle, stated early last year that "[l]egislation is going to have to happen unless industry can convince all those people up on the Hill that it's not needed."[170] To date, it appears that none of the Internet privacy issues have actually been resolved by legislation or by the ecommerce industry itself. Unfortunately, then, that means I have no clear-cut answer for those of you concerned about your online privacy rights. Until federal regulators and members of the e-commerce industry agree that the issue of online privacy will not be resolved without both groups' active participation and regulation, all of us Web users and consumers are forced to keep all eyes open to the technology we applaud, and fear.[171]

*Courtenay Youngblood*

170 McCullagh & Morehead, *FTC Goes Public with Privacy*, WIRED NEWS NETWORK, Dec. 10, 2000, *available at* http://www.wired.com/news/politics/0,1283,37695,00.html.

171 On March 29, 2001, U.S. District Judge Naomi Rice Buchwald of the U.S. District Court for the Southern District of New York said that DoubleClick was not engaged in the secret collection of private and personal data from Internet users. In dismissing a class action lawsuit against DoubleClick, Inc., the court held that the placing of "cookies" on a computer user's hard drive by an Internet advertising agency is not an invasion of privacy. (*See*, Michael A. Riccardi, *DoubleClick Wins Dismissal of Suit Alleging "Cookies" Harmed Web Users*, N.Y. LAW .J., Mar. 30, 2001, at 1).